INTERNATIONAL JOURNAL OF MATHEMATICAL SCIENCES AND APPLICATIONS
Volume 5 • Number 1 • January-June 2015

DESIGN OF IDENTITY BASED CRYPTOGRAPHIC SCHEMES FROM PAIRING

Rajeev Kumar[1], S.K. Pal[2] and Arvind[3]

[1]Dyal Singh College, University of Delhi, Delhi, India, E-mail: rajeev82verma@gmail.com, [2]DRDO, Delhi, India, E-mail: skptech@yahoo.com, [3]Hansraj College, University of Delhi, Delhi, India, E-mail: arvind_ashu12@rediffmail.com

Abstract*: In Public Key Cryptography, each person owns a pair of key, one is called the public key and other the private key. The public key is published and used for encryption, while the private key is kept secret and used for decryption of messages. The need for the sender and receiver to share secret information is eliminated: all communications involve one's public key and the private key need not be shared. However, generation of such key pairs is computationally complex and requires substantial computing infrastructure. Moreover, linking a large random public key with an individual has been a practical problem since the invention of public key cryptography.*

Identity based Encryption (IBE) is an exciting variant of public-key encryption, as it eliminates the need for a Public Key Infrastructure (PKI). The sender using an IBE scheme does not need to look for the public keys and the corresponding certificates of the receivers. IBE uses identities for generation of public keys. One of the most successful ways of designing ID based schemes is by use of pairing. In this paper we present Identity Based Encryption schemes using Bilinear Pairings over elliptic curves. We describe how bilinear pairings (Weil or Tate pairing) over super-singular elliptic curves may be used to construct Identity Based Encryption schemes. We also present digital signature schemes derived from pairings having shortest known signature lengths at typical security levels.

Keywords*: Public key cryptography, elliptic curve, Weil pairing, Identity Based Encryption, Signature Scheme.*

1. INTRODUCTION

In a public key or asymmetric cryptosystems [1] there are two keys. The public key which is published in a directory allows encryption and the private key which is kept secret allows decryption. Public key cryptography was publicly introduced by Whitefield Diffie and Martin Hellman in 1976. Ronald Rivest, Adi Shamir and Leonard Adleman proposed a scheme in 1977, which became the most widely used public key cryptographic scheme, RSA. ElGamal cryptosystem is a non-RSA public key cryptosystem based on discrete logarithms.

In public key cryptography pair of key is either generated by the user or by some central authority. In the latter care, a secure channel is needed to transport the key pair to the user. So generation of such key pairs is computationally complex and requires substantial computing infrastructure. It is practically very difficult to link a large random public key with an individual key. We need Public Key Infrastructure (PKI) for it.

The first use of elliptic curves for cryptography [2] was suggested independently by Koblitz and Miller in 1985. Elliptic curve cryptography (ECC) provides the same level of security as RSA or discrete logarithm systems with considerably shorter operands. ECC is becoming accepted as an alternative to cryptosystems such as RSA and ElGamal over finite fields. Super singular curves played an important role to make the first fully functional identity based cryptosystem.

2. IDENTITY BASED ENCRYPTION

Identity based encryption (IBE) is an important primitive of ID-based cryptography. It is a type of public-key encryption in which the public key of a user is some unique information about the identity of the user.

In 1984, Shamir [3] invented the concept of Identity-Based Encryption, which addresses the authenticity problem of public keys in a different way. His idea was to avoid the need for authentication altogether, by making sure that the actual value of a user's public key is inherently linked to his identity. More precisely, a user can use his/her identity as the public key, which simplifies the key management procedure compared to certificate-based cryptosystem. The RSA scheme did not be used in this manner to satisfy the conditions implemented by Shamir which are not present in RSA. Shamir proposed the digital signature and encryption in his work but he admitted that the security of his encryption scheme is still an open problem.

Recall that in conventional public-key cryptosystems, key pairs are generated by randomly choosing a secret key and applying some one-way function to compute the public key. But in ID-base cryptography, first of all the public key is uniquely determined by the identity of user, instead of computed from the secret key. The secret key needs to be derived from the public key, instead of the other way around. To generate the secret key, there is a third party in environment, called key generation centre (KGC). The KGC is able to do this, because that has the privilege of knowing some master information, called the "master" key. So a user's secret key is than computed as some one-way function of the public key and the master key. If we assumed that there is a sender 'A' at one end and on the other side there is a receiver say 'B'. Then both of these parties trust on the third party (KGC) for secrecy. Suppose 'A' wants to send an encrypted message to 'B'. For this first KGC creates an environment by providing the keys to 'A' and 'B'. 'A' gets the public master key using his own private ID (it may be Bank ATM's Pin number, email address, phone number etc). After this 'A' is authenticated by the KGC and receive the private key. By getting these keys 'A' executes the encryption process and finally protected message is transferred to 'B'. Before applying the decryption and verification process, 'B' gets the master public key from KGC using his ID and also KGC authenticate it to provide the private key. Now 'B' can decrypt and verify the actual message.

An ideal ID-based encryption would satisfy the following properties [4]:

1. Users only need to know the identity of the user they want to communicate with.
2. There is no need for keeping public directories such as files with public keys of certificates.
3. The services of the KGC are needed only during the system in set up phase.

One of the major advantages of any identity-based encryption scheme is that if there are only a finite number of users, after all users have been issued with keys the third party's secret can be destroyed. This can take place because this system assumes that, once issued, keys are always valid. Moreover, as public keys are derived from identifiers, IBE eliminates the need for a public key distribution infrastructure. The authenticity of the public keys is guaranteed implicitly as long as the transport of the private keys to the corresponding user is kept secure.

An IBE scheme can be described using the following four steps in a cycle:

Setup: In first step, program generates the global system parameters and a master key.

Extract: After setup, in next step it generates private key which correspond to an arbitrary public key string ID by using the master key.

Encrypt: Now it encrypts the message using the public key ID.

Decrypt: At last it decrypts the message using the corresponding private key.

An Identity-Based Signature (IBS) scheme can be described in the steps: Setup, Extract, Sign and verify.

We are illustrating schematic outline of IBE and IBS schemes:

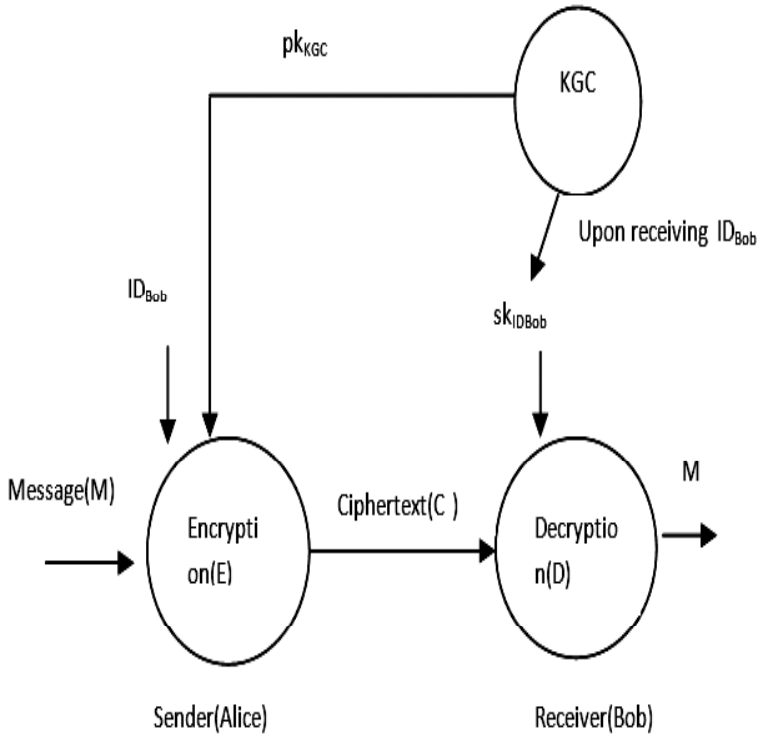

Figure 1: Identity-Based Encryption

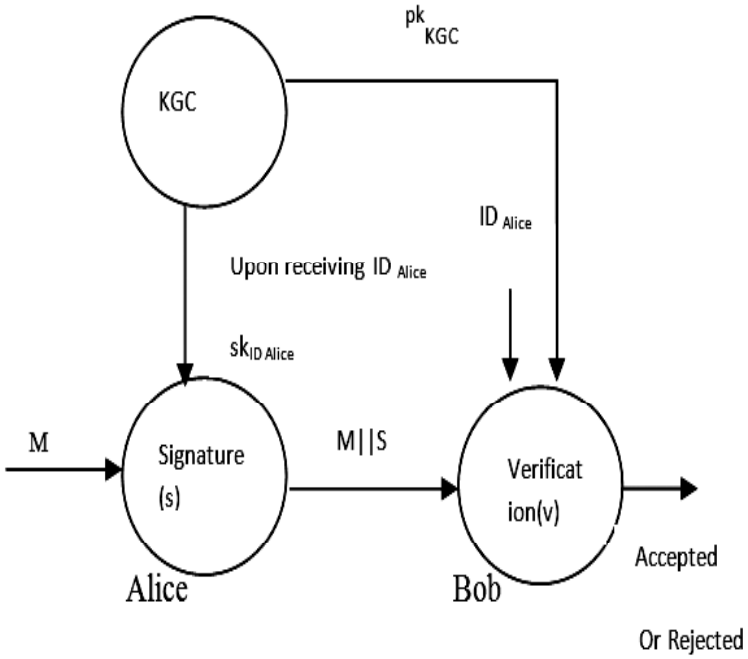

Figure 1: Identity-Based Signature

In 2001, Boneh and Franklin provided the solution of the open problems raised by Shamir in his IBE scheme in 1984. They developed a fully functional Identity-Based Encryption scheme [5] by using pairing on Elliptic Curves. After this scheme, pairing has become one of the most attractive topics in cryptography. Many IBE and IBS schemes were developed by using pairing. The most efficient identity-based encryption and signature schemes are currently based on bilinear pairings on elliptic curves.

3. CRYPTOGRAPHIC PAIRING

A pairing or bilinear map [6] in elliptic curve cryptography is a mapping that takes as input two points on an elliptic curve and outputs an element of a multiplicative abelian group.

Let G_1 be an additive cyclic group generated by P, whose order is a prime q, and G_2 be a multiplicative group of the same order q. A bilinear pairing is a map $e : G_1 \times G_1 \rightarrow G_T$ with the following properties:

1. Bilinear: $e(aP, bQ) = e(P, Q)^{ab}$, for all $P, Q \in G_1$ and for all $a, b \in Z_q^*$.
2. Non-Degeneracy: There exists $P \in G_1$, such that $e(P, P) \neq 1$.
3. Computable: There is an efficient algorithm to compute $e(P, Q)$ for all P, Q ? G_1.

This is the first form of pairing. The second form of pairing used in the cryptography literature is

$$e : G_1 \times G_2 \rightarrow G_T$$

where G_1, G_2, G_T are groups of prime order say l. This is also bilinear and non-degenerate. We always use the second form and consider the first form to be just the special case $G_2 = G_1$. Galbraith, Peterson, and Smart [7] classify the pairings into the following three types based on the concrete structures of the underlying groups:

Type I: if $G_1 = G_2$;

Type II: if $G_1 \neq G_2$ but there is an efficiently computable homomorphism $\Phi : G_2 \rightarrow G_1$;

Type III: if $G_1 \neq G_2$ but there is no efficiently computable homomorphism between G_1 and G_2.

Shacham introduced a new kind of pairing in his PhD thesis. According to this definition, suppose G_1 and G_T are cyclic groups of prime order say n,G_2 is taken to be a group of exponent n, whose order is some power of n. This pairing was later called a Type IV pairing.

Bilinear pairing is an important cryptographic primitive and has been widely adopted in many positive applications in cryptography. Many cryptosystems have been designed using bilinear pairings. In this section, we also briefly recall the definition of the Weil pairing and Tate pairing.

Let $K = F_q$ be a finite field with $q = p^n$ elements, where p is prime and let E be an elliptic curve defined over F_q. The point at infinity is denoted by O.

3.1 Weil Pairing

Let m be a fixed integer coprime to p and let $P, Q \in E[m]$. Let A and B be divisors such that $A \sim (P) – (O)$ and $B \sim (Q)–(O)$, and A and B have disjoint support. Since P and Q are m-torsion points, it follows that mA and mB are principle divisors. So there are rational functions $f_P, f_Q \in \bar{K}(E)$ such that $div(f_P) = mA$ and $div(f_Q) = mB$, with these notions, the Weil pairing [6]

$$e_m : E[m] \times E[m] \rightarrow \mu_m$$

is given by:

$$e_m(P,Q) = \frac{f_P(B)}{f_Q(A)}.$$

The Weil pairing e_m as defined above is well defined i.e. maps to a m^{th} root of unity and is independent of the choice of A and B and functions f_P and f_Q. This e_m is also bilinear and non-degenerate.

3.2 Tate Pairing

Let m be a positive integer coprime to q, such that $E(F_q^k)$ contains a point of order m. Let k be the smallest integer satisfying $m|q^k - 1$. Suppose $K = F_q^k$. Let $P \in E(K)[m]$, then $m(P) - m(O)$ is a principal divisor. So we get a rational function $g \in K(E)$ such that $div(g) = m(P) - m(O)$. Now let Q be a point from $E(K)/\ mE(K)$, then we construct a divisor D of degree zero such that $D \sim (Q) - (O)$. Support of this D should be disjoint from the support of the divisor of g. With these notations, the Tate pairing [8]

e: $E(K)[m] \times E(K)/mE(K) \rightarrow K^* / K^{*m}$,

is given by : $e(P, Q) = g(D)$.

This pairing is also bilinear and non-degenerate. The output of this pairing is only defined up to a coset of K^{*m}, however for protocols we will require a unique element of K^*. Hence to obtain a unique representative, one defines the reduced Tate pairing as

$$e(P,Q) = g(D)^{(q^k-1)/m}$$

If the function g in the above definition is normalized, i.e. $(u_o^m g)\,(o) = 1$ for some F_q-rational uniformizer u_O at O, then one can ignore working with the divisor D and simply can work with the point Q, *i.e.* the reduced Tate pairing is

$$e(P,Q) = g(Q)^{(q^k-1)/m}$$

For every $P \in E(K)$ and integer s, let $f_{s,P}$ be an K-rational function with divisor

$$div\,(f_{s,p}) = s(P) - ([s]P) - (s-1)O.$$

Such function $f_{s,P}$ is called Miller function and determined uniquely up to multiplication by non-zero elements of K. With this rational function, the above definition can be written as

$$e(P,Q) = f_{m,P}(Q)^{(q^k-1)/m}.$$

4. CONSTRUCTION OF IBE USING PAIRING

Boneh and Franklin [5] developed an IBE scheme in the flavour of ElGamal that rests squarely on the shoulders of a particular supersingular curve and a slightly modified version of the Weil pairing. They introduced two encryption schemes BasicIdent and FullIdent. The BasicIdent scheme is useful as a teaching tool, but is not suited for practical use because its security guarantees are too weak for most applications. Therefore, Boneh and Franklin convert the BasicIdent scheme into the FullIdent scheme, called fully functional IBE, which provide stronger notion of security. For a concrete implementation of their scheme they propose to use the modified Weil pairing on the supersingular elliptic curve $y^2 = x^3 + 1$ over F_p, where $p > 3$ is a prime such that $p \equiv 2 (\mathrm{mod}\, 3)$. The version FullIdent of IBE is as follows:

Setup: on input of a security parameter k, the algorithm works as follows:

1. Generate a random k-bit prime q such that $q \mid p + 1$, and $q^2 \mid p + 1$. After that we generate two groups $(G_1, +)$, $(G_2,*)$ of order q ($G_1 = E(F_p)$ $[q]$, $G_2 = \mu_q$), and a symmetric pairing $e : G_1 \times G_1 \rightarrow G_T$. We choose an arbitrary generator $P \in G_1$.
2. Pick a random $s \in \mathbb{Z}_q^*$ and set public key $P_{pub} = sP$.
3. Choose cryptographic hash functions $H_1: \{0,1\}^* \rightarrow G_1^*$, $H_2 : G_T \rightarrow \{0, 1\}^n$, $H_3: \{0,1\}^n \times \{0,1\}^n \rightarrow \mathbb{Z}_q^*$ and $H_4: \{0,1\}^n \rightarrow \{0,1\}^n$ for some n.

The message space is $M = \{0,1\}^n$ and the ciphertext space is $C = G_1^* \times \{0,1\}^n \times \{0,1\}^n$. The system parameters are params = $<q, G_1, G_T, e, n, P, P_{pub}, H_1, H_2, H_3, H_4>$. The master key is $s \in \mathbb{Z}_q^*$

Extract: For a given string $ID \in \{0, 1\}^*$ the algorithm works as follows:

1. Compute $Q_{ID} = H_1 (ID) \in G_1^*$.
2. Set the secret key d_{ID} to be $d_{ID} = sQ_{ID}$, where s is the master key.

Encrypt: To encrypt the massage $M \in M$ under the public key ID, the algorithm work as follows:

1. Compute $Q_{ID} = H_1 (\text{ID}) \in G_1^*$.
2. Choose a random $\sigma \in \{0, 1\}^n$, .
3. Set $r = H_3 (\sigma, M)$ and set the ciphertext to be $C = <rP, \sigma \oplus H_2 (g_{ID}^r), M \oplus H_4(\sigma) >$, where $g_{ID} = e(Q_{ID}, P_{pub}) \in G_T$.

Decrypt: Let $C = <U, V, W>$ be a cipher text encrypted using the private key ID. To decrypt C using the private key $D_{ID} \in G_1^*$, the algorithm works as follows:

1. Compute $V \oplus H_2(e(d_{ID}, U)) = \sigma$
2. Compute $W \oplus H_4(\sigma) = M$
3. Set $r = H_3 (\sigma, M)$. Check whether $U = rP$, if not, reject the cipher text.
4. Output M as the decryption of C.

The above four steps design an efficient encryption scheme.

5. DIGITAL SIGNATURE USING PAIRING

Digital signatures are one of the most important information security services offered by public key cryptography. Since 1984, several practical Identity Based Signature (IBS) schemes have been proposed, but no satisfactory IBS scheme appeared till 2001. In 2001, when Boneh and Franklin cleverly used bilinear pairing over super singular elliptic curves in their scheme, a number of ID-based signature schemes have been proposed. In 2003, Cha and Cheon [9] presented an IBS scheme from Gap Diffie-Hellman Groups. This scheme consists of four algorithms as follows:

Setup: It is similar as in IBE. In addition we pick a hash function $H_5 : \{0, 1\} \times G \rightarrow \mathbb{Z}_q^*$.

Extract: It is similar as in IBE.

Sign: To sign a message M with secret key d_{ID}, the algorithm works as:

1. Pick a random $r \in \mathbb{Z}_q^*$.

2. Compute $U = rQ_{ID}, h = H_5(M, U),$ and $V = (r + h)Q_{ID}$.

3. Set the signature to be $\sigma = (U, V)$.

Verify: Now to verify a signature $\sigma = (U, V)$ on a message M, we check whether $e(P, V) = e(P_{pub}, U + hQ_{ID})$, where $h = H_5(M, U)$.

This is the complete description of the scheme. Cha and Cheon proved that their schemes are secure against existential forgery under adaptive chosen message and fixed ID-attack in the random oracle model with assumption that the CDH problem is intractable.

Boneh, Lynn and Shacham [10] also used pairings to construct a signature scheme in which the signatures are rather short. With the exploit of bilinear pairings several efficient and secure ID-based signature schemes have been proposed till now.

6. CONSTRUCTION OF EFFICIENT IBE SCHEME

In 2001, the first Identity-Based Encryption scheme using groups with efficiently computable bilinear maps was introduced by Boneh and Franklin. After their work many IBE schemes with different security model was given by the researchers. Boneh and Boyen [11] provided a practical IBE scheme in the selective-ID model. Waters [12] provided an efficient and fully secure system without random oracle model under the decisional Bilinear Diffie-Hellman (BDH) assumption. In 2010, Xia Fei, Yanqin Zhu and Xizhao Luo [13] developed an Efficient Identity Based Signature scheme in the standard model. This scheme is without random oracles and they prove that it achieves adaptive identity, chosen plaintext security. Compared with other IBS schemes, this scheme has comparable properties and computation efficiency.

Chih-Hung Wang and Chao Chuan Chen [14] provided an identity-based concurrent signature scheme from bilinear pairing with improved accountability. The concept of the concurrent signature was introduced by Chen, Kulda and Paterson. Concurrent signature provides a new idea for fair exchange without the help of the trusted third party. Only two parties interact to produce two signatures. The scheme proposed by Wang and Chen can resist message substitute attack and achieve the property of real accountability.

P.V.S.S.N. Gopal, P. Vasudeva Reddy, T. Gowri [15] proposed a new ID-based signature scheme using bilinear pairings over elliptic curves. They proved that this scheme is secure against existential forgery under adaptively chosen message and ID attack in random oracle model with the assumption that the computational Diffie-Hellman problem is intractable. Recently, G. Swapna, P. Vasudeva Reddy and T. Gowri [16] proposed an Efficient Identity Based Multi-Proxy Multi-Sign encryption scheme using bilinear pairing over elliptic curves. This scheme is both verifiable and forward secure. The security of the proposed scheme is based on the Computational Diffie-Hellman problem. They proved that their scheme requires less number of pairing computation as compared to previous schemes.

Yijun Mao, Xi Zhang, Min-Rong Chen and Yiju Zhan [17] provided a constant size hierarchical identity based encryption tightly secure in the full model without random oracles. This scheme is fully secure where ciphertext size and decryption cost is constant, and the security reduction is tight regardless of the hierarchy depth and the number of private key queries. The assumption of their system is a new one, less natural and less well-studied than decisional BDH.

7. SECURITY ANALYSIS

Following the paper, presented by Boneh and Franklin in 2001, many identity-based cryptographic schemes, based on bilinear pairings from supersingular elliptic curves were proposed. The public key generation in many of these schemes is simple and similar, merely the hash value of each user's publicly known identity. A general statement is given in these schemes that the hash functions used must be cryptographic strong. Traditionally, a hash function is said to be cryptographic strong if it satisfied the four properties: easy forward computation, pre-image resistance, second pre-image resistant and collision. Jyh-Haw Yeh [18], provided a simple hash function satisfying the above four properties, but the resulting identity-based schemes are insecure, where private keys can be easily derived from public keys. He defined an additional derivable cryptographic hashing property, image ratio resistance, to hash functions for identity-based cryptosystems. He also showed that the identity-based cryptosystems without this hashing property are potentially insecure.

If we divide all existing identity-based encryption schemes, which make use of pairing, into four categories (Type I schemes with Type I pairing, Type II schemes with Type II pairing and so on). We shall see that a number of efficient and secure schemes can be implemented in Type III schemes, or less efficiently in the Type II schemes. The rest are implementable only in the Type I and Type IV schemes. In Type I schemes we have problems due to efficiency as the security parameter increases as we are restricted to supersingular curves. Current research indicates that at higher security levels, Type I pairings are expected to be slower on many platforms. In Type IV schemes the security proofs become more cumbersome as the image of the hash function into G_2 is not going to be into the group generated by P_2. So Type II and Type III are considered better choices. Because of the reduced cost of pairing evaluation and also the relatively smaller size of elements of G_2, Type III is overall better choice.

8. CONCLUSION

In this paper we presented the Identity Based Encryption (IBE) schemes using bilinear pairings over elliptic curves. We described how Weil or Tate pairing over supersingular elliptic curves may be used to construct these schemes. We have elaborated on digital signature schemes derived from pairings. IBE is a new research area in pairing based cryptography. A lot of efforts have been put in finding pairing-based applications of IBE. Nevertheless, we believe that IBE has many interesting applications in store. We plan to work on new constructions for IBE for its use in present day applications over mobile & constrained environments.

REFERENCES

[1] W. Diffie, M. Hellman, "Directions in Cryptography", *IEEE Transactions on Information Theory*, 22 (1976), pages 644-654.

[2] V.S. Miller, "Use of Elliptic Curves in Cryptography", *Advanced in Cryptology-Crypto*, 85 pages 417-426, Springer-Verlag, New York, 1985.

[3] I.A. Shamir, "Identity-Based Cryptosystems and Signature Schemes", *Advances in Cryptology-Crypto'84*, LNCS 1233, Springer- Verlag, pages 47-53, 1984.

[4] A.J. Menezes, Van Oorschot, P.C. and S.A. Vanstone, "Handbook of Applied Cryptography", CRC Press, 1996.

[5] D. Boneh and M. Franklin, "Identity-Based Encryption from the Weil pairing", *Advances in Cryptology-Crypto* 2001, LNCS 2139, Springer- Verlag, pages 213-229, 2001.

[6] Ben Lynn, "On the Implementation of Pairing-Based Cryptosystems", 2007.

[7] S. Galbraith, K. Paterson and N. Smart, "Pairings for Cryptographers, Discrete Applied Mathematics", **156**, pages 3113-3121, 2008.

[8] Martijn Mass, "Master's Thesis on Pairing-Based Cryptography", Technische Universiteit Eindhoven, 2004.

[9] J. Cha and J. Cheon, "An Identity-based Signature from Gap Diffie-Hellman Groups, in: PKC' 03, LNCS 2567, Pages 18-30, Springer-Verlag, 2003.

[10] D. Boneh, B. Lynn and H. Shacham, Short Signatures From Weil pairing, Advances in Cryptology- Asiacrypt 2001, LNCS 2248, Springer-Verlag, pages 514-532, 2003.

[11] D. Boneh and X. Boyen, "Efficient Selective-ID Identity Based Encryption without Random Oracles", *Advances in Cryptology-Euro Crypt 2004*, 3027, pages 223-238, Springer-Verlag, 2004.

[12] B. Waters, "Efficient Identity Based Encryption without Random Oracles", *Advances in Cryptology-Euro crypt 2005*, **3494**, pp. 114-127, Springer-Verlag, 2005.

[13] Xie Fei, Yanqin Zhu and Xizhao Luo, "Efficient Identity Based Signature Scheme in the Standard Model", *Advanced Computer theory and Engineering (ICACTE)*, IEEE, 2010.

[14] Chin-Hung Wang and Chao Chuan Chen, "Identity Based Concurrent Signature Scheme with Improved Accountability", *Computer Society*, IEEE, 2011.

[15] P.V.S.S.N. Gopal, P. Vasudeva Reddy and T. Gowri, "New Identity Based Signature Scheme using Bilinear Pairing Over Elliptic Curves", *IEEE*, 2012.

[16] G. Swapna, P. Vasudeva Reddy and T. Gowri, "Efficient Identity Based Multi-Proxy Multi-Signcryption Scheme using Bilinear Pairing Over Elliptic Curves", ICACCI, IEEE, 2013.

[17] Yijun Mao, Xi Zhang, Min-Rong Chen and Yiju Zhan, "Constant Size Hierarchical Identity-Based Encryption Tightly Secure in the Full Model without Random Oracles", ICEIDWT, IEEE, 2013.

[18] Jyh-Haw Yeh, "Security Vulnerability in Identity-Based Public Key Cryptosystems from Pairings", *International Journal of Information and Education Technology*, **3**, 2013.